Submission to PJCIS Inquiry into the
National Security Legislation Amendment Bill (No.1) 2014
Authority and immunity for ASIO officers to engage in unlawful conduct

The attached discussion paper "the role of the intelligence function in a Westminster system of governance" highlights divergent perspectives on the primary role of the intelligence function in a liberal democracy. The first "executive action" intelligence paradigm is largely exemplified by the (paramilitary) operations of the CIA and some other foreign services. The second paradigm defines intelligence as a professional and independent advisory and decision-support function, and this has largely been the defensive and constrained role played by ASIO since its transformation following the Justice Hope inquiries in the 1970s and 1980s. Since that time the scope of ASIO's operations have been circumscribed by legislation and a comprehensive oversight regime, and national security priorities have been determined through an objective and transparent risk management process.

There is no doubt that 9/11 has transformed the security environment, typified by a militarist response to perceptions of the threat of terrorism. Since 9/11 there have been persistent calls for a relaxation of the constraints on the operations of security-related organisations, for the integration and convergence of previously separate (intelligence/police/military) functions, and for a utilitarian shift towards a more offensive "executive action" operational role, all in the name of counter-terrorism.

The proposal under Division 4 of the new NSLA Bill to give ASIO officers the authority and immunity to engage in unlawful conduct as part of "special intelligence operations" appears to give effect to the goal of removing essential controls on the covert operational activities of that organisation, potentially broadening ASIO's executive action role and fundamentally changing the nature of the organisation. ASIO's primary role has been to provide Government with high quality independent advice, with the Government taking responsibility for deciding whether or not to act on such (inherently fallible) advice. If the Government decides that administrative or legal or enforcement action is justified it tasks the appropriately authorised professional body (such as the Australian Federal Police). While the separation of the intelligence and law enforcement functions in the counter-terrorism area can pose particular challenges in terms of the use of sensitive information and intelligence in legal processes, it recognises the fundamental difference between (secret) intelligence and (public) evidence and protects officials involved in state-sanctioned criminal activities.

Division 4 in the Bill on special intelligence operations proposes significant criminal sanctions against anyone who discloses the details of sensitive covert activities. Does this mean that intelligence officers involved in a special intelligence operation that inadvertently led to someone's death could be obliged to conceal the crime? Who decides what reporting and accountability mechanisms would apply to officers involved in murky criminal conduct? Would a jury in a criminal trial of an alleged terrorist be informed that the intended attack was ASIO-organised? Anyone who has worked for any time in sensitive operational roles knows that the ultimate safeguard against zealous, incompetent or irresponsible covert action is the professionalism and integrity of individual officers who feel empowered to speak out.

ON LINE *opinion* - Australia's e-journal of social and political debate

Terrorism and the power of fear

By Bill Calcutt
Posted Wednesday, 11 June 2014

Fear is a visceral human emotion with the power to overwhelm and subsume all other feelings and rational thoughts. Terrorism seeks to coerce political and social change by threatening extreme and indiscriminate violence against the community. But the real power of terrorism is not the capacity of zealots to threaten or undertake violence but its ability to catalyse an extreme and disproportionate reaction from the state, effectively perpetuating and magnifying the community's fear and changing the nature of society. Terrorism relies for its enduring impact on the state (over)reacting in ways that permanently transform perceptions of national security. By responding to terrorism in expedient, oppressive and inhumane ways the state can erode its own democratic principles and moral authority, ultimately weakening social cohesion.

Terrorism has a unique capacity to undermine democracy by eliciting a militaristic response that suspends or compromises a number of the important conventions and principles of civil society, including democratic accountability. This is because the secrecy that invariably surrounds national security makes it virtually impossible for the community to determine whether counter-terrorism actions are justified and proportionate to a real (rather than exaggerated) threat, and to hold elected representatives to account.

Almost thirteen years ago a small group of terrorists hatched an audacious and improbable plan to take spectacular violent action that they hoped would be a catalyst for change in the course of human history, not unlike the assassination of Archduke Ferdinand in 1914 that ignited the Great War. Against virtually insurmountable odds terrorists managed to strike at global symbols of Western civilization by crashing commercial planes into several iconic buildings in the United States, igniting a war on terror.

The immediate tactical goal of the terrorists was to damage and humiliate the world's sole superpower. Their longer-term strategic goal was to catalyse fundamental social change by increasing community insecurity and engendering a disproportionate war-like response. The terrorists could only dream of triggering an enduring transformation of national and global security priorities with a shift towards an authoritarian and utilitarian approach in security-related policy, the militarisation and privatisation of civilian functions, and a realignment of the balance between national security and individual and civil rights.

In the period since 9/11 the terrorists have succeeded in achieving these strategic goals beyond their wildest dreams. Several wars have been undertaken at enormous human and financial cost. A large covert paramilitary apparatus, unconstrained by the laws of war, has been established with the capacity to strike virtually anywhere in the world. Billons have been spent on security measures world-wide, including developing the technical capability to monitor anyone and everyone, anywhere.

Human rights are increasingly defined by national citizenship, with certain classes of "non-citizens" no longer entitled to the protection of the rule of law.

Inexplicably, many of our political leaders tacitly participate in the continuing distortion of the threat of terrorism, and the perpetuation of the myth of the paternalistic state. They do so through their implicit acceptance that "national security" is inviolate and the security sector can and should be trusted to operate beyond the bounds of democratic oversight and accountability. Few leaders are apparently willing to publicly discuss and question the paradigm shift that has occurred in national security over the last decade, with the extension of the secret state with implications for many of the institutions that are central to a robust and progressive democracy.

Why have otherwise advanced, sophisticated and civilised societies responded to the actual threat of terrorism in these extreme and sometimes undemocratic ways? One possible explanation is that developed states actually need an existential threat to maintain their own identities in the face of an increasingly diverse and heterogeneous global community. In the period since the end of the cold war a number of developing nations have flourished, transforming geopolitical dynamics and challenging the West's economic and military hegemony. The interdependencies created through globalisation are progressively breaking down traditional distinctions between nations, challenging centuries-old concepts of sovereignty, national identity and Western exceptionalism.

Another possible explanation is that, post 9/11, the interests of a now extensive and resurgent security sector have become deeply entrenched and highly influential. The end of the cold war precipitated a progressive shift of resources and power away from the defence and security sectors as countries increasingly focussed on competing globally in a relatively stable world. At the same time many countries reduced state secrecy and increased transparency, reinforcing civil liberties and adopting a broader objective risk-based approach in determining national security priorities. After 9/11 the defence and security sectors moved quickly to reassert their preeminent role as the unquestioned protectors of the state, and secrecy displaced transparency as the default position in public oversight and disclosure relating to national security.

There is great irony that there is an alignment of the interests of terrorists threatening indiscriminate violence with those whose mission is to defend the state's security, both of whom benefit from the community's ongoing fear and insecurity. In the altered post 9/11 security environment Australians have been willing to tolerate a range of exceptional security measures including the extension of video and electronic surveillance; the blurring of the roles of civilian, policing and military functions; increasing the powers of the security agencies; the removal of the right to legal recourse for some non-citizens; and the criminalisation of associations rather than activities. More recently border security has been militarised, with the covert deployment of paramilitary forces to protect against the perceived threat of drugs, guns, pests and asylum seekers.

Bill Calcutt worked in a range of intelligence roles in the Australian Security Intelligence Organization and the National Crime Authority from the early 1970s till the mid 1990s.

Eureka Street – Vol 23 No 15

Civil liberties in a grave new world

Bill Calcutt - 08 August 2013

Since the Second World War Western democracies have championed human rights, decrying the abuse of civil liberties in undemocratic states. A defining feature of the Cold War was trenchant Western criticism of the pervasive surveillance of citizens in authoritarian Eastern Bloc states. In stark contrast Western democracies took great care in seeking to balance national security and civil liberties, often reflected in detailed legislation circumscribing the powers of intelligence agencies and upholding the rights of individuals.

Australia operates under a Westminster system of democratic governance that is intended to provide checks and balances against the concentration and abuse of power. Justice Robert Marsden Hope showed great foresight in crafting Australia's unique intelligence architecture, institutionalising the separation of information collection and analysis, national and foreign intelligence, and advisory and decision-making functions.

While Hope recognised that national security agencies need to operate under the cloak of secrecy to be effective, he established mechanisms to ensure proper oversight and accountability. He emphasised the intrinsic fallibility of intelligence advice (intelligence always involves an element of interpretation and subjectivity) and its limited utility as evidence in legal proceedings or as the sole basis for executive action.

Since the turn of the millennium three major technology-enabled developments have significantly altered the balance between national security and civil liberties. The first is that virtually universal access to information and communication technology has empowered individuals and groups to communicate and organise. This development, most graphically illustrated in the social revolutions in the Middle East (the Arab Spring), seems to represent the disaggregation of power from traditional state institutions to the broader community and diverse media outlets.

The second development is that technology has dramatically increased the capacity of the state to remotely surveil its citizens under the aegis of national security. As revealed by US National Security Agency contractor Edward Snowden, ubiquitous electronic linkages and a largely unregulated cyberspace make it technically possible for the state to monitor and collect virtually every single piece of personal digital data created knowingly or unknowingly by every citizen, potentially rending existing legislative frameworks regulating national security activities obsolete.

The third and arguably most significant development has been the rise of the threat of international terrorism, with violent individuals or groups able to engender global fear through the leverage of extensive real-time media

coverage. Terrorism explicitly seeks to elicit a disproportionate state response, catalysing major social and political change. The 'global war on terror' in response to 9/11, and the threat posed by Al Qaeda, effectively shifted the focus of national security activities in many countries to counter-terrorism. Under emergency 'wartime' conditions, traditional civilian/peacetime constraints on military and intelligence activities are largely subsumed.

In fact the threat of international terrorism was perceived as so serious that many long-standing international conventions governing the treatment of lawful combatants, use of torture, resort to extra-judicial killing, exceptional rendition and incarceration without trial were suspended.

In pursuit of terrorists, new military technologies have been developed enabling precision/surgical strikes against military and intelligence targets using remote-controlled drones or special operations forces. States have developed paramilitary capabilities that can be deployed covertly virtually anywhere in the world, unconstrained by the international laws of war. Recent revelations indicate that states have also developed powerful global surveillance capabilities under the auspices of counter-terrorism.

Australia's counter-terrorism responses post 9/11 have been significant. Beyond the commitment of military forces to conflicts in Iraq and Afghanistan, expenditure on our intelligence capabilities has quadrupled over the last decade to over $1.4 billion. At the same time the legislation governing the operations of the intelligence agencies has been amended to add additional powers to respond to prospective terrorism threats.

It seems likely that a number of the careful security/liberties balances institutionalised by Hope have been compromised in a utilitarian response to the threat of terrorism. Pressures for the integration of military, police and intelligence functions and for the inclusion of secret intelligence as evidence in public legal proceedings directly challenge the essential checks and balances that are an integral part of Hope's intelligence model.

As noted earlier the goals of terrorism are to engender widespread fear and a disproportionate state response. In Australia counter-terrorism has proved to have powerful political connotations. Fear has great political currency here, and any suggestion of weakness on national security (or law and order) can be political poison.

This intense environment has made temperate and informed public discourse on appropriate risk-based national security priorities difficult, particularly in the context of the secrecy, misinformation and sense of urgency that inevitably accompanies consideration of counter-terrorism issues. Counter-terrorism remains a potent rationale for many of the state's most secret activities, with ongoing demands from agencies for additional resources and unfettered access to increasing circles of data.

The hyper-politicisation of national security finds voice in the current discourse on the issue of border security, turning a complex humanitarian and policing

challenge (asylum seekers arriving by sea) into an enormously controversial and expensive imbroglio. Government has legislated to add the protection of border integrity from serious threats to the definition of security, potentially enabling the deployment of intelligence and military resources against people desperately seeking humanitarian refuge in this country.

Bill Calcutt worked in a range of intelligence roles in the Australian Security Intelligence Organization and the National Crime Authority for more than twenty years. More recently he has worked as an associate lecturer is postgraduate security studies at an Australian university. He retains a strong interest in governance, ethics and accountability.

Discussion Paper

The role of the intelligence function in a Westminster system of governance

Introduction

Why are there so many divergent and confusing perspectives in the literature on the purpose and essential elements of the intelligence function? Possible reasons include:

- A generally poor understanding of the nature of national security
- Widely divergent perspectives on the nature of the intelligence function and its role within a national security system
- Misconceptions about what constitutes intelligence product
- The sensationalist and distorted portrayal of the intelligence function in popular culture and the media
- The secrecy that inevitably accompanies most intelligence activities
- Differences within the intelligence community on priorities and methodology
- Imprecision in the use of the term “intelligence” (semantic confusion).

Contemporary discourse on the intelligence function reflects the complexity and diversity of views on these issues. Because the intelligence function’s primary purpose is to covertly support the State’s exercise of power, in addition to protecting advantage there may some official reluctance to reveal some (utilitarian) activities that may be perceived as being on the margins of broader social and legal norms.

Making sense of the many perspectives on intelligence can be challenging, so the aim of this discussion paper to tease out some key concepts to provide readers with a foundation for critical analysis, discussion and reflection. These observations necessarily reflect the authors’ backgrounds in national security and criminal intelligence, and a number of the issues addressed are widely contested.

National security and risk management

Under the "social contract" the State has a fundamental obligation to its citizens to provide an orderly and secure environment. In return for the State's protection, citizens are obliged to eschew resort to force, except in self-defence.

National security refers to the protection of the institutions and interests of the State from potential internal and external threats. The Australian Government's 2009 Defence White Paper states "National security is concerned with ensuring Australia's freedom from attack or the threat of attack, maintaining our territorial integrity and promoting our political sovereignty, preserving our hard-won freedoms, and sustaining our fundamental capacity to advance economic prosperity for all Australians".

In an increasingly complex security environment many Governments have adopted an objective risk management approach to determining their national security priorities. Risk management examines and compares the probability and consequences of a diverse range of potential risks in order to identify those that pose the greatest relative threat (in terms of political, social and economic costs).

The Australian Government's 2008 National Security Statement broadens the scope of the Government's risk management approach to recognise "all hazards". This approach identifies a broad range of potential risks, ranging from the traditional threats of espionage and terrorism to contemporary issues like pandemics, climate change and transnational crime. Under this approach, national security is accepted as a broad Government responsibility (managing diverse risks), with the intelligence function playing a specific and clearly defined role in advising on actual and potential threats.

The failure to comprehensively implement an effective risk management approach to national security is starkly revealed through an examination of the September 11 attacks. Commercial airlines had previously been subject to hijack during the 1970s, but the subsequent deregulation of the airlines industry throughout the 1980s resulted in a relaxation of security measures. In the September 11 attacks terrorists

were able to seize control of several planes and turn them into powerful missiles because of the failure of the risk management process to:

- Detect and respond to a threat of plane hijacks
- Identify and address the potential vulnerability of plane cockpits
- Recognise the potential of planes as missiles
- Recognise the potential consequences of missiles directed at strategic targets.

Divergent national perspectives on the nature of the intelligence function

It is important to understand that not every State defines its national security interests in the same way. The nature of the intelligence function will depend on the State's conceptions of the scope of its national security interests. This is best illustrated through a comparison of the approaches of the United States and Australia. The US defines national security in a very broad way, reflecting its substantial global interests and capabilities as a superpower. As a consequence the intelligence function is an integral (albeit secret) element of US foreign policy.

In contrast to many other Western countries, the US is virtually unique in not having a dedicated domestic security intelligence organization. This has its origins in the US Constitution and the associated principles concerning protection of the rights and liberties of US citizens. National security is the primary responsibility of the Federal Bureau of Investigation (FBI), whose traditional focus has been law enforcement and foreign counter-intelligence. There have been significant changes in US domestic intelligence arrangements since September 11, including the establishment of a Department of Homeland Security and major changes to FBI tasking and priorities.

The Central Intelligence Agency (CIA), which is constrained by law from operating domestically, operates around the world (often in concert with the US military) to advance the US's national security and foreign policy interests. The CIA's role reflects a number of unique American imperatives:

- Perceptions of the US's global interests and responsibilities as a superpower

- US administration views on the nature of external threats to US interests, and the options available to respond to these threats (including resort to force)
- A conviction that decisive and unilateral action can be taken overseas to neutralize threats to the US, based on a right to pre-emptive self defence
- A significant paramilitary/covert operations capability
- A concentration of executive authority in the hands of the US President.

This discussion highlights the existence of two markedly different intelligence paradigms. The first paradigm, discussed above, defines intelligence as **covert State action aimed at foreign powers.** The main characteristics of this "executive action" model of intelligence are:

- A primary focus on external (foreign) threats to strategic interests
- International sphere of interest & operations ("global reach")
- Predominantly an offensive role based on concept of pre-emptive self-defence
- Strong emphasis on supporting military/war-fighting operations
- A heavy reliance on technology & real-time tactical support
- Clear distinction between rights of citizens & non-citizens
- National security & global security are intertwined
- Executive authority & international law
- Intelligence-military continuum
- Advisory-policy continuum.

There are powerful national and cultural dimensions to this paradigm, reflecting deeply-embedded convictions about the primacy of US national interests, the moral legitimacy and imperative of exercising (super) power globally, and the international legal authority of pre-emptive self-defence. This unique US perspective is referred to by various commentators as "American exceptionalism".

Some commentators have contended that major intelligence failures are more likely under the executive action model because:

- The world is so huge, complex, dynamic and unpredictable that it is simply not feasible from a resource or technology perspective to sustain the extensive

coverage required to detect and monitor all potential threats across the globe. Kevin O'Connell notes the belief that US intelligence can be omniscient

- There is an inherent contradiction between viewing all potential risks and threats as foreign/external/other, while neglecting to safeguard against potential internal/domestic threats to security
- Combining the advisory and policy/political functions inevitably compromises the quality and independence of the intelligence advice produced.

In contrast to the US's broad conception of its global security interests and reach, many countries define their primary national security interests as the protection and defence of the sovereign State against a range of internal and external threats. The national security function in these States is thus primarily defensive, and relates to internal issues such as safety, protection, order and social cohesion. The role of the intelligence function in this context is primarily limited to the provision of high quality independent advice to government on prospective internal and external threats to national security in order to support executive decision-making.

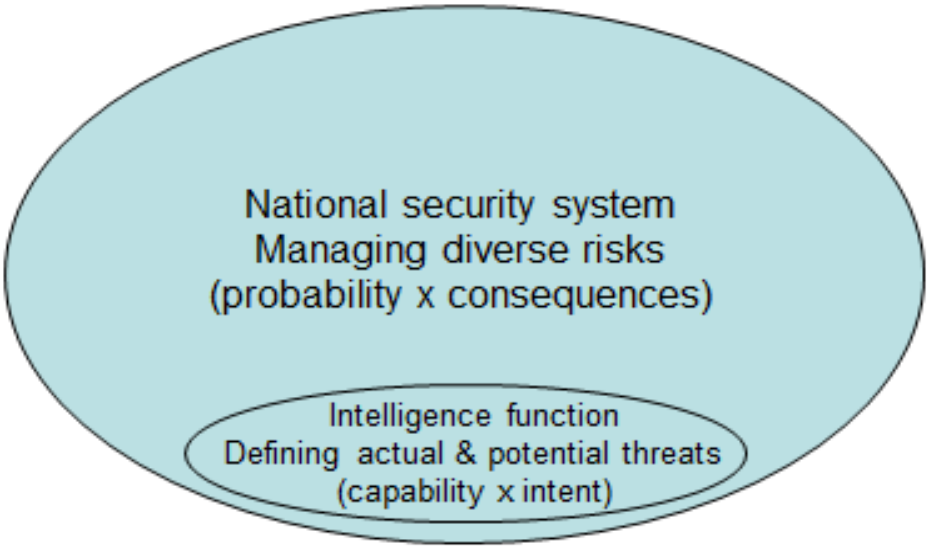
In those States that are founded on the Westminster system of governance, the post-war articulation of an autonomous intelligence process (cycle) was explicitly intended to cast the intelligence function as an independent advisory and decision-support capability that is structurally separate from government. The intelligence process institutionalises the subordinate relationship between an intelligence function (the independent adviser) and the state (the decision-maker), encapsulating the Westminster principle of the separation of powers and formalising the checks and balances that ensure accountability and safeguard against the abuse of power.

The second dominant paradigm therefore defines intelligence as **a professional and independent advisory and decision-support function** to Government on prospective threats to national security**.** The main characteristics of this Westminster model of intelligence are:

- National (domestic) sphere of operations (protect the sovereign state)
- Predominantly a defensive role
- Dedicated national security organisation

- Risk management approach to potential threats
- Functional separation of advisory & policy roles (independence)
- Balance between rights of citizens & powers of the State
- Clear statutory limits, national accountability & oversight.

Under the Westminster model, independent intelligence advice can make a valuable contribution to the risk management process by providing input on the capability and intent dimensions of particular threats, and can thus enhance and support national security decision-making by reducing uncertainty and increasing options. In Westminster countries (like Australia) the relationship between the intelligence function and the national security system is reflected in the diagram below.



In Australia, the application of the Westminster principles (of structural separation) has had significant implications for the organisation and operations of the Australian Intelligence Community. The principles are reflected in the separation of the collection and analytical agencies, the separation of the domestic security intelligence and foreign intelligence functions, and significantly different (more stringent) regulatory regimes covering activities that impact on Australian citizens.

Misconceptions about what constitutes intelligence product

The marked divergence in national views about the role of the intelligence function is matched by a pervasive misunderstanding of what actually constitutes intelligence product, and a consequent imprecision in the use of the term “intelligence”. The term is used variously (and loosely) to describe information that is collected secretly or that emanates from sensitive sources; information of value; unique insights derived from the rigorous analysis and interpretation of incomplete information.

This latter type of product has particular value because it adds meaning through the application of inductive and abductive reasoning to information. For the purposes of this paper intelligence product is defined as “insights and understanding on current and prospective threats that, in the absence of factual data, can inform and enhance decisions on actions to anticipate and manage risk” (or simply “insights that provide direction for effective action”). Under this definition, intelligence is a unique high quality product that can offer decision-makers the advantage of forewarning, but remains inherently fallible due to the elements of interpretation and prediction. The best analogy is a jigsaw, where only parts of the puzzle are available but the analyst has to try and describe the whole picture.

There is a major difference in terms of a level of probability between a hypothesis and intelligence product. A hypothesis is speculation on possibilities that can be the start of a journey of inquiry. There is no qualified level of probability attached to a hypothesis, it can be entirely conjecture. In contrast, intelligence product represents the best informed judgement, a specified level of probability, and the application of rigorous analytical skills (a form of inductive logic). The crucial skill in intelligence analysis (the key accountability for the analyst) is the acuity to develop unique insights that provide direction for effective action.

Professional intelligence analysis has a number of important characteristics:

- Intellectual rigor
- Critical thinking
- Discipline
- Objectivity

- Independence

in the examination and testing of what is known or can be reasonably inferred, and in the development of insights on and understanding of trends and patterns &

- Creativity
- Innovation
- Imagination
- Foresight

in the development of forecasts about the future.

The intelligence analyst's primary task is to determine and report the probable truth in the absence of all the facts (referred to in some of the literature as "speaking truth to power"). There are a range of unique personal and professional characteristics required to undertake this type of work:

- Constant scepticism
- A commitment to professionalism and intellectual integrity
- The confidence to provide an independent (sometimes unpopular) perspective
- A willingness to accept the limits of an advisory role (others make decisions)
- A willingness to play a secondary role to operational functions
- A willingness to accept personal responsibility for perceptive judgements
- A willingness to acknowledge the inherent fallibility of intelligence assessments, and on occasion accept that conclusions are flawed.

Generic performance indicators for intelligence product include:

- Timely
- Relevant & actionable
- Independent & objective
- Thorough & inclusive of all relevant information
- Disciplined in its careful representation of information
- Distinguishes between information & inferences
- Stipulates an explicit level of probability
- Demonstrates foresight & ultimately proves accurate.

Media depiction of the intelligence function

The public's perceptions, misconceptions and expectations of the intelligence function (and intelligence activities) are significantly shaped by the typically sensationalist and distorted portrayal of the function in popular culture and the media. The public's main exposure to intelligence is either the stereotype "spook" that reflects (atypical and usually fictional) dangerous, deceptive or violent roles, or extensive media reporting of intelligence "failures" (sometimes following major official inquiries such as WMD and September 11).

The constraints of secrecy

The secrecy that surrounds (in conjunction with the often sensationalist media depiction of) intelligence activities mean that there are many public misconceptions about the role of an intelligence function in a liberal democracy. Secrecy is not a necessary prerequisite for intelligence activities, but is a typical element.

A huge amount of information is now available publicly (referred to as open source information) and intelligence assessments are often based on information from both public and covert sources. Information is collected covertly to avoid alerting subjects of interest to an investigation; to conceal sensitive human sources and technical capabilities; and to protect the advantage of forewarning. Activities of interest to the State are often deliberately concealed by the perpetrators (espionage, conspiracy), and covert collection is sometimes the only way of obtaining directly relevant information.

People who work in intelligence roles accept a principle called "need to know" that is intended to limit the disclosure and dissemination of sensitive information and ensure its protection. Sensitive information is typically classified according to its level of protection – confidential, secret, top secret. People who handle classified information are vetted by the Australian Government Security Vetting Agency and given clearances to access sensitive information up to a particular level. Even with security clearances "need to know" prevails.

Secrecy can impose major constraints on effectiveness in a number of ways. It can limit sharing and essential co-ordination within and between relevant agencies (observations of the September 11 inquiry, and a growing recognition that "need to know" needs to be balanced against "need to share"); it can inhibit the development of broader and more accurate perspectives by restricting the consideration of potentially relevant (sometimes contradictory) information; it can prevent the use of classified material in important public discourse and policy development; and it can impede the critical scrutiny of the justification for action (ensure accountability).

It is worth making a clear distinction between secret information and intelligence product, and their potential for use as evidence in legal or administrative processes. Evidence is information that is admissible in a court and whose veracity as fact can be (normally publicly) tested. There are occasions where secret information may potentially be admissible as factual evidence, and in such circumstances the question that has to be decided is whether continuing protection (of sensitive sources or methods) takes precedence over the value and use of the secret information as evidence.

In contrast to secret information, intelligence product cannot be represented as fact as it contains judgements and interpretations (is inherently fallible), and is thus more difficult to publicly test (rarely viable for an analyst be called as an "expert" witness).

Differences within the intelligence community on priorities and methodology

Despite an obvious commonality of purpose, historically there have been significant differences within the Australian Intelligence Community (and within individual agencies) on what are the most important stages of the intelligence process, and what are the unique skills and capabilities required for particular types of intelligence activities. These differences in emphasis invariably reflect individual agencies' primary focus (security, foreign, criminal, military) and specialist roles (technical, operational, collection, analysis, strategy).

There can be tension between operational "coal face" investigators (including covert information collectors) and head office "desk" analysts whose role is to take a

broader perspective and critically evaluate information from diverse sources. Officers who task information collection can sometimes be oblivious to the difficulties of and unique expertise required for covert information collection (particularly in roles dealing with the management of human sources). There can also be a divergence between technical information collection agencies that feed raw data directly into high level decision-making processes (with little analysis), and those agencies that subject covertly obtained information to critical analysis in order to qualify and add value for decision makers.

The two Hope Commission reports (the 1977 Royal Commission on Intelligence and Security and the 1985 Royal Commission on Australia's Security and Intelligence Agencies) highlighted the central role of analysis in transforming raw information into valuable intelligence product. Justice Hope stressed the importance of separating the collection and analysis functions in order to protect the objectivity of analysis and maximise the independence of the resultant intelligence product. Likewise Justice Hope emphasised the importance of subjecting the domestic security intelligence function to a much higher and more rigorous level of regulation and accountability than the foreign intelligence function. These key principles, designed to institutionalise important checks and balances on the operations of Australian intelligence agencies, were (re)affirmed in the 2011 Independent Review of the Intelligence Community (IRIC) report.

Imprecision in intelligence terminology (semantic confusion)

The term **intelligence** is used variously (sometimes indiscriminately) to refer to:

- An **industry** or profession
- **Covert State action aimed at foreign powers** (executive action model)
- **A professional and independent advisory and decision-support function** (Westminster model)
- An iterative and sequential **process** that has a number of distinctive parts, involving the planned and systematic collection, processing and analysis and synthesis of information, and the subsequent dissemination of the resultant intelligence product. Also referred to as the "intelligence cycle" to reflect the fact it is a feedback loop

- A unique type of **rigorous analysis** (cognitive process) that interprets and transforms raw information into a high quality intelligence product
- The output or **product** of the intelligence process, comprising insights, interpretations and predictions that support decision-making by reducing uncertainty and broadening options. Because this advice includes an element of interpretation it remains inherently fallible
- **Covertly obtained information**. Under this definition anything that is collected secretly qualifies as intelligence product
- **Any useful or valuable information.**

The 2011 Independent Review of the Intelligence Community (IRIC) report defines intelligence as “information that enables you to protect your interests or to maintain a valuable advantage in advancing your interests over those posing a threat to them”. The report notes that this definition does not distinguish how the information is collected or whether it is secret, but that it “confers an advantage through superior insight or the fact you are in possession of information when others are not”. Appendix 1 to the IRIC report states “any helpful definition of intelligence has to go well beyond the collection and dissemination of useful information”.

Conclusion

This discussion paper has sought to disentangle and simplify a number of the conceptual and definitional issues that typically surround discourse on and the study of the intelligence function. The paper places the intelligence function squarely in a broader governance context as a unique, secret but independent government function that can make a valuable contribution to the effectiveness of the national security risk management process.